Evaluation Report

FY 2001 DOD INFORMATION SECURITY STATUS FOR GOVERNMENT INFORMATION SECURITY REFORM

Report No. D-2001-184 September 19, 2001

Office of the Inspector General
Department of Defense

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

September 19, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Evaluation Report on FY 2001 DoD Information Security Status for Government Information Security Reform (Report No. D-2001-184)

We are providing this summary report for your review. This summary report was made in compliance with the requirements of the Government Information Security Reform Act, title X, subtitle G of the FY 2001 Floyd D. Spence National Defense Authorization Act (Public Law 106-398). The public law requires an independent assessment of each Department's information security posture based on a review of a subset of systems and other audits and evaluations of information security conducted during the reporting period. No written response to this report is required.

Questions on this report should be directed to Ms. Wanda A. Hopkins at (703) 604-9049 (DSN 664-9049) (wahopkins@dodig.osd.mil), Mr. Robert K. West at (703) 604-8983 (DSN 664-8983) (rwest@dodig.osd.mil), or Ms. Judith I. Padgett at (703) 604-8990 (DSN 664-8990) (jpadgett@dodig.osd.mil). See Appendix F for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Acting Assistant Inspector General
for Auditing

Additional Copies

To obtain additional copies of this evaluation report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Evaluations

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Evaluation Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AIS	Automated Information System
CIO	Chief Information Officer
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
GISRA	Government Information Security Reform Act
IT	Information Technology
NIPRNet	Non-secure Internet Protocol Router Network
OMB	Office of Management and Budget

Office of the Inspector General, DoD

Report No. D-2001-184 September 19, 2001
Project No. D2001AD-0071.002

FY 2001 DoD Information Security Status for Government Information Security Reform

Executive Summary

Introduction. The Government Information Security Reform Act (the Act) directs each Federal agency to evaluate its information security program and practices annually and, as part of the budget process, submit the results to the Office of Management and Budget. The Act covers unclassified and national security systems and creates the same security management framework for each. The Act establishes parallel requirements for the agency and the agency Inspector General. Specifically, the Act requires DoD to annually evaluate its information security program and practices and confirm their effectiveness by testing a subset of systems. The Act also requires the Office of the Inspector General to evaluate the DoD information security program and practices and to independently select and test a subset of systems to confirm the effectiveness of the information security program.

Objectives and Scope. The overall objective was to respond to the requirements of the Government Information Security Reform Act, title X, subtitle G of the FY 2001 Floyd D. Spence National Defense Authorization Act (Public Law 106-398). The Office of the Inspector General, DoD, selected an independent subset of applications to assess the effectiveness of DoD information security policy and practices. The Army Audit Agency and the Air Force Audit Agency supported the Office of the Inspector General, DoD, in that review. In addition, the Office of the Inspector General, DoD, identified and summarized information security and information assurance concerns from April 1, 2000, through August 22, 2001. The subset results, the information assurance report summary, and the Army Audit Agency and Air Force Audit Agency specific discussion of the questions posed by the public law form the basis of our results.

Results. Although DoD has made progress in developing various information assurance initiatives, DoD still needs to establish and implement a DoD-wide information security plan to better manage and coordinate collective efforts by the DoD Components in protecting and defending DoD systems and networks. The results that follow appear with the corresponding number from the Office of Management and Budget reporting guidance. The guidance requires the Office of the Inspector General, DoD, to respond to questions 2 through 13.

2. Identify the total number of programs included in the program reviews or independent evaluations.

The Office of the Inspector General, DoD, the Army Audit Agency, and the Air Force Audit Agency collaborated on a review of a subset of applications resident on the Defense Information Systems Agency-owned Centers and Detachments. The statistical sample randomly selected from that subset was 90 of 1,365 applications, organized by unique names from a total population of 4,939 applications. The Defense Enterprise Computing Centers and Detachments support multiple DoD Components, installations, and functions. The applications support functions that include financial accounting; personnel; pay and disbursement; materiel shipping, receiving, and storing; munitions maintenance; and weapon systems.

3. Describe the methodology used in the program reviews and the methodology used in the independent evaluations.

To assess the information technology security posture of DoD, the Office of the Inspector General, DoD, selected a random sample of business applications from a subset of systems. For those applications, the objective was to identify security personnel, such as the Information System Security Officer and the Designated Approval Authority, and to determine whether the applications had a Certification and Accreditation or an Interim Authority to Operate.

4. Report any material weakness in policies, procedures, or practices as identified and required under existing law.

Of 49 reports summarized in Inspector General, DoD, Report No. D-2001-182, "Information Assurance Challenges—a Summary of Audit Results Reported April 1, 2000, through August 22, 2001," September 19, 2001, 23 reports identified weaknesses in policies, procedures, or practices concerning information assurance. Thirteen reports specified that the control weaknesses identified were material.

5. Describe the specific measures of performance used to ensure program officials have: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques. Include information on the actual performance for each of the four categories.

The DoD integrated assessing risk, identifying appropriate security level, maintaining a current security plan, and testing and evaluating security controls and techniques into its DoD Information Technology Security Certification and Accreditation Process program. Based on the results of our review of the subset of systems from the Defense Enterprise Computing Centers and Detachments, DoD had not fully implemented security policy. Written, current certification and accreditations were not available for an estimated 60 percent of the subset population of 1,365 applications. Certification and accreditation are the technical evaluation of security features of an application or

system and the formal declaration to operate the application or system. The DoD managers had not fully implemented information security policy because definitions for system, application, and other means of establishing security parameters and responsibilities were unclear. The parameters of and responsibility for information security were made more complex by the DoD practice of approving different organizations to design, develop, manage, use, and operate information technology applications.

6. Describe the specific measures of performance used to ensure that the CIO: 1) adequately maintains an agency-wide security program; 2) ensures the effective implementation of the program and evaluates the performance of major agency components; and 3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories.

Although DoD Directive 5200.28 specifically assigns oversight and review for implementation of its stated policies to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), the Assistant Secretary had no mechanism in place to provide that oversight. Additionally, the directive assigns responsibility to DoD Component heads for implementing and ensuring compliance with the directive, and for programming funds and resources to support information security. The DoD Components also had no mechanisms for comprehensively measuring compliance with DoD Directive 5200.28. The Assistant Secretary also had not established a DoD enterprise information security plan to consistently apply information assurance to all DoD systems and networks. Further, the changing information technology environment made it difficult to maintain current security policies and practices.

7. Describe how the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training were available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training.

The Office of the Inspector General, DoD, did not identify the total number of DoD employees who required information security training, the types of security training available during the reporting period, the number of DoD employees who received each type of training, or the total costs of providing training. Specifically, the Office of the Inspector General, DoD, observed, in Report No. D-2001-182, that the DoD was progressing towards its information assurance training and certification requirements. DoD established the Human Resources Development Functional Area to develop and institute the means to continually improve education, training, and awareness of personnel required to carry out the DoD information assurance mission.

8. Describe the documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the

General Services Administration's FedCIRC. Include information on the actual performance and the number of incidents reported.

Prior audit and investigative coverage showed that, although the DoD was making progress in reporting and investigating security incidents, additional improvements were needed. Inspector General, DoD, Report No. D2001-013, "DoD Compliance With the Information Assurance Vulnerability Alert Policy," December 1, 2000, evaluated the DoD procedures for reporting security incidents and sharing information about common vulnerabilities. The report stated that DoD had made significant progress towards implementing its procedures and planned to be fully compliant by April 2001. However, as of August 31, 2001, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) had not issued a formal instruction, identified the positions and skills needed by the primary and secondary points of contact, or issued an implementation plan for the Information Assurance Vulnerability Alert process. The Army Audit Agency noted that the Army improved its information security posture by establishing the Army Computer Emergency Response Team and the Information Assurance Vulnerability Alert Compliance Verification Team.

In the area of computer crime, in FY 2001, the Defense Criminal Investigative Organizations (the Army Criminal Investigation Command, the Naval Criminal Investigative Service, the Air force Office of Special Investigations, and the Defense Criminal Investigative Service) initiated 194 investigations, closed 178 investigations, had 24 indictments and 18 convictions, and recovered and avoided costs of $2.9 million.

9. Describe how the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY02 capital asset plan (as well as exhibit 53) submitted by the agency to OMB? If no, why not?

The Office of the Inspector General, DoD, cannot comment on whether DoD reported security requirements and costs on every FY 2002 capital asset plan or exhibit 53 submitted to the Office of Management and Budget because it did not examine those plans. However, the Army Audit Agency reviewed some aspects of capital planning and investment that it reported in Report No. AA 01-284, "Workload Survey for Information Technology," May 31, 2001. Specifically, the Army Audit Agency reported that the Army had an Investment Strategy Working Group that prioritized information technology investments and aligned the Army's portfolio of systems with its requirements.

10. Describe the specific methodology used to identify, prioritize, and protect critical assets within the enterprise architecture, including links with key external systems. Describe how the methodology has been implemented.

The Office of the Inspector General, DoD, did not specifically review a methodology used by the DoD to identify, prioritize, and protect critical assets within its enterprise architecture. However, the Office of the Inspector General, DoD, identified the need

to improve contingency planning and certification and accreditation efforts. Those are areas that help DoD protect critical assets and information.

11. Describe the measures of performance used by the head of the agency to ensure that the information security plan is practiced throughout the life cycle of each system. Include information on the actual performance.

The DoD Information Technology Security Certification and Accreditation Process, according to DoD Instruction 5200.40, applies to all life-cycle phases of DoD systems. The DoD did not have a means of evaluating and consolidating information assurance data to report the DoD information security posture, as evidenced by results from the Inspector General review of the selected subset of applications. That review showed 60 percent of the 1,365 applications did not have current certifications and accreditations made by using the DoD Information Technology Security Certification and Accreditation Process or any other assessment tool.

12. Describe how the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs.

The Office of the Inspector General, DoD, participated in the Joint Task Force—Computer Network Defense and the National Infrastructure Protection Center programs. Both programs contribute to the protection of critical infrastructure assets and information.

13. Describe the specific methods used to ensure that contractor-provided services or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy.

Audits are one method DoD uses to help identify weaknesses in the acquisition policies and procedures for information technology services. Five reports, by the Office of the Inspector General, DoD, and the Air Force Audit Agency, identified weaknesses with contractor-provided information technology services. One of the weaknesses identified was the failure to require security investigations of contractor employees, including foreign nationals, prior to the employees writing software code for critical systems. In addition, those reports documented commercial packages that did not have adequate controls to safeguard sensitive financial information and contracts that did not have adequate contract administration for security requirements.

Recommendations to Improve the Government Information Security Reform Reporting Process. The Office of the Inspector General, DoD, recommends that the Office of Management and Budget take the following actions to improve the process of responding to the Government Information Security Reform Act.

- Carefully define terminology in future reporting guidance. Interpretations of the terminology used to discuss information security varied and resulted in responses about very different things. Terms that were subject to interpretation

and extensive debate included system, application, network, mission-critical, and mission-essential. The guidance needs to define the terminology to the extent necessary for comparable discussions.

- Clarify what the agency should evaluate for information security. The debate on terminology extends to the items that an agency should consider in evaluating information security. The guidance should specify that all information technology investments are included. Further, the distinction between national security systems and all other systems should be discontinued to facilitate consistent information security coverage.

- Improve the timing of guidance and responses. Guidance on the specific information that the agencies should include in their reports to the Congress needs to be available at the beginning of the reporting year. The official Government Information Security Reform reporting guidance was not available until late June 2001 for a reporting date of October 1, 2001. Changes to the questions for discussion for the next reporting period need to be available before the agencies plan and accomplish the reviews to provide responses to the Government Information Security Reform Act requirements. If the Government Information Security Reform Act continues to require the Inspector General, DoD, to report results from audits of independent evaluations on national security systems, the Office of Management and Budget should initiate a legislative request to establish a separate reporting period for national security systems. That reporting period should allow sufficient time for the audit function to validate the results of the independent evaluations.

Table of Contents

The Inspector General, DoD, Response to Address the Government Information Security Reform Act

General Provisions of Government Information Security Reform. On October 30, 2000, the President signed the Defense Authorization Act of FY 2001 (Public Law 106-398) that included title X, subtitle G, "Government Information Security Reform" Act (GISRA). Subtitle G provides for ensuring effective controls for highly networked Federal information resources, management and oversight of information security risks, and a reporting mechanism for improved information system security oversight and assurance for Federal information security programs. The GISRA directs each Federal agency (the DoD for purposes of this report) to evaluate its information security program and practices annually and, as part of the budget process, submit the results to the Office of Management and Budget (OMB). The GISRA covers unclassified and national security systems and creates the same security management framework for each.

DoD and Inspector General Provisions of GISRA. The GISRA establishes parallel requirements for the agency and the agency Inspector General. It requires DoD to annually evaluate its information security program and practices and confirm their effectiveness. GISRA also requires the Office of the Inspector General to independently evaluate the DoD information security program and practices, and select and test a subset of systems to confirm the effectiveness of the information security program.

The Subset Selected by the Office of the Inspector General. The Office of the Inspector General, DoD, selected its independent subset of systems from the applications supported by the Defense Enterprise Computing Centers (the Centers) and Detachments of the Defense Information Systems Agency (DISA). As of February 2001, DISA billed its customers to run 4,939 applications, comprising 1,365 unique-named applications, that became the source of the subset sample. We chose a random sample of 90 applications from the population of 1,365. The Army Audit Agency evaluated 34 applications and the Air Force Audit Agency evaluated 19 applications supporting their respective Components. The Office of the Inspector General, DoD, evaluated the balance of 37 applications, which supported the Navy, the Defense Finance and Accounting Service, and the Defense Logistics Agency.

OMB Guidance and Reporting Instructions for GISRA. The OMB issued guidance implementing GISRA in memorandum M-01-08, "Guidance on Implementing the Government Information Security Reform Act," January 16, 2001. That guidance broadly outlined responsibilities within agency structures for evaluating and reporting information security.

On June 22, 2001, the OMB issued the memorandum 01-24, "Reporting Instructions for the Government Information Security Reform Act," that it directed to the heads of executive departments and agencies. Memorandum 01-24 provides instructions for completing the executive summary required by the GISRA. OMB directed agency Chief Information Officers (CIO) and program

officials, including the DoD, to respond to 14 comprehensive questions described in the memorandum. Each agency Inspector General would respond to questions on the results of its independent evaluation of the agency's information security status except those questions concerning the total information security funding and the strategy to correct security weaknesses.

Sources of Support for GISRA Reporting Requirements. A primary source of support for our responses to the OMB questions was the evaluation of the independently selected subset from the applications operating at the DISA Centers and Detachments. The Army Audit Agency and the Air Force Audit Agency contributed significantly to that evaluation. In addition, those audit agencies provided the Office of the Inspector General, DoD, with responses to the OMB questions for their respective Components. (See Appendix C for the Army Audit Agency responses and Appendix D for the Air Force Audit Agency responses.) Reports, evaluations, and information collected for the period from April 2000 through August 2001 from the following sources were also used to develop the responses: General Accounting Office; Office of the Inspector General, DoD, Army Audit Agency, Naval Audit Service, and Air Force Audit Agency.

We did not validate the DoD responses to the OMB questions because the DoD and the Office of the Inspector General, DoD, concurrently collected and evaluated data and developed separate responses to submit to OMB.

We could not obtain comprehensive information to respond to all of the OMB questions. In keeping with the January 16, 2001, OMB memorandum, we selected a subset of systems from the business applications operated at the DISA Centers and Detachments to test the effectiveness of the DoD security program and practices. In our overall response, we also used those audits, evaluations, and inspections completed during FY 2001 that addressed information security. We were unable to plan the reviews to respond specifically to the OMB questions because those questions were not available until June 2001.

Recommendations to Improve the GISRA Process. The experience gained in responding to GISRA requirements for the first time highlighted some opportunities to improve the process. Our recommendations for the OMB are in the following discussion.

Carefully Define GISRA Terminology. Interpretations of the terminology used to discuss information security varied and resulted in very different responses to GISRA requirements and OMB questions. For example, the OMB guidance asked that the agency identify the total number of programs included in the program review. The Air Force Audit Agency interpreted program to mean operational programs, such as the Air Force Materiel Command system, "Programmed Depot Maintenance Scheduling System (GO97)." In contrast, the Army Audit Agency interpreted program to mean functional areas of interest such as the Army-wide security program, "Network Security Improvement Program (sustaining base)." Other terminology that was subject to interpretation and extensive debate included system, application,

network, mission-critical, and mission-essential. We believe OMB needs to define the terminology to the extent necessary for comparable topic discussions.

Clarify What the Agency Should Evaluate for Information Security. The debate of terminology extended to the items that an agency should consider in information security evaluations. Interpretations also varied on whether GISRA applied to non-mission-critical and non-mission-essential weapons systems, communications networks, business systems, and Information Technology (IT) funded outside the DoD IT Registry requirements. We believe that OMB should clarify its guidance to include all IT investments. Further, we believe that the distinction between national security systems and all other systems should be discontinued to facilitate consistent information security coverage.

Improve the Timing of Guidance and Responses. The OMB needs to issue guidance on the specific information that the agencies should include in their reports to OMB and Congress at the beginning of the reporting year. The official GISRA reporting guidance was not available until late June 2001, which left insufficient audit lead time because of the firm reporting date of October 1, 2001. Changes to the questions for discussion for the next reporting period need to be available before the agencies plan and accomplish the reviews to provide responses to the GISRA requirements. If GISRA continues to require the Inspector General, DoD, to report results from audits of independent evaluations on national security systems, OMB should initiate a legislative request to establish a separate reporting period for national security systems. That reporting period should allow sufficient time for the audit function to validate the results of the independent evaluations.

Background

The DoD IT Universe. The DoD has thousands of IT processes that comprise its IT universe. One can categorize those processes according to a variety of criteria, including function, criticality, locality, and owner or operator. Two categories or populations identified in DoD for the FY 2001 GISRA review were the IT Registry systems and the business applications supported by the Centers, for which DISA billed its customers. Some of those Center-supported processes or applications were also included in the IT Registry, though not all were.

IT Registry Database of Systems. Public Law 106-398, section 811, "Acquisition and Management of Information Technology," requires DoD to register all mission-critical and mission-essential IT systems with the DoD CIO in the IT Registry. To obtain funding, a system must be in the IT Registry. The IT Registry requires 17 data fields, including system name, description, functional area, and program manager information. As of August 30, 2001, DoD Components registered 3,783 unclassified IT systems with the CIO.

Center-Supported Applications. The Centers and Detachments of DISA provided general support systems, including mainframe computers,

minicomputers, and local area networks, for its customers' applications. Each Center operates under the control of the Center commanding officer, with system security functions accomplished by the designated security manager and the information systems security manager. The DISA has five Centers that are located in Mechanicsburg, Pennsylvania; Columbus, Ohio; St. Louis, Missouri; Oklahoma City, Oklahoma; and Ogden, Utah. In addition, there are Detachments or satellite sites at 14 other locations. The Center customers are the Military Departments and other Defense agencies with installations throughout the United States. The customer applications that the Centers and Detachments run to support DoD installations include financial accounting; personnel; pay and disbursement; materiel shipping, receiving, and storing; munitions maintenance; and weapon systems.

The DoD Information Security Program. The primary document establishing the DoD information security program is DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, which provides the mandatory, minimum security requirements for automated information systems (AISs) based on acceptable levels of risk. Directive 5200.28 has several companion regulatory and procedural documents, including DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," (DITSCAP), December 30, 1997.

The DITSCAP Program. DoD Instruction 5200.40 implements DoD Directive 5200.28; it prescribes procedures to accomplish policy goals and establishes standards for certifying and accrediting the security of DoD IT systems throughout their life cycles.

Objectives

The overall evaluation objective was to respond to the GISRA requirements of title X, subtitle G of the FY 2001 Floyd D. Spence National Defense Authorization Act (Public Law 106-398). We did not evaluate the management control program separately because the DoD recognized information security and assurance programs as a material weakness in its most current Statement of Assurance. In addition, the GAO identified information security as a high risk. See Appendix A for a discussion of the evaluation scope and methodology. See Appendix B for prior coverage related to the evaluation objectives.

Responses to Questions on Government Information Security Reform

The results correspond with the numbered questions from OMB reporting guidance. The guidance requires the Office of the Inspector General, DoD, to respond to questions 2 through 13.

2. Identify the total number of programs included in the program reviews or independent evaluations.

The Office of the Inspector General, DoD, the Army Audit Agency, and the Air Force Audit Agency collaborated on a review of a subset of systems from the applications resident at the DISA-owned Centers and Detachments. The statistical sample that we randomly selected from that subset was 90 of 1,365 applications, organized by unique names from a total population of 4,939 applications. The statistical sample of 90 applications reviewed resulted in a projected point estimate to the population of 1,365 for authority to operate as follows:

	Projected Results	Percent of Population
Current Certification and Accreditation or Interim Authority to Operate	501	36.7
Indeterminate: retired, transferred, insufficient detail available to find status	410	30.0
Other technology with no Certification and Accreditation or Interim Authority to Operate	137	10.0
Expired Certification and Accreditation or Interim Authority to Operate	30	2.2
No Certification and Accreditation or Interim Authority to Operate, or certification only	288	21.1
Total	**1,366**[1]	**100.0**

The Centers and Detachments support multiple DoD Components, installations, and functions. The applications provide support to functions that include financial accounting; personnel; pay and disbursement; materiel shipping, receiving, and storing; munitions maintenance; and weapon systems.

[1] The projected point estimates do not add up to the population of 1,365 due to rounding.

In addition to reviewing the subset, the Office of the Inspector General, DoD, compiled results reported in audits, evaluations, and GAO testimony. Those results, reported in Report No. D-2001-182, "Information Assurance Challenges-A Summary of Audit Results Reported April 1, 2000, through August 22, 2001," September 19, 2001, were from the Inspector General, DoD, the General Accounting Office, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency. We used that compilation to discuss some of the questions in the OMB reporting guidance. The compilation included reports that discussed security for 22 IT investments, including networks and systems for specific user requirements (for example, Air Force Research Laboratory UNIX-based computer systems, the Integrated Accounts Payable System, and the Advanced Logistics Program).

The DoD selected its systems for evaluation from a different source than the Office of the Inspector General. The DoD selected a statistical sample from the systems listed in the IT Registry. We did not validate the data collected by DoD. Although the evaluations were of different subsets of systems, both subsets provide an overview of the complexity and diversity of the DoD IT.

3. Describe the methodology used in the program reviews and the methodology used in the independent evaluations.

To assess the IT security posture of DoD, we selected a random sample of applications from a subset of systems. For those applications, the objective was to identify security personnel, such as the Information System Security Officer and the Designated Approval Authority, and to determine whether the applications had a security Certification and Accreditation or an Interim Authority to Operate. See Appendix A for details of the sample and methodology.

We obtained additional information for reporting by reviewing reports and testimony from the Office of the Inspector General, DoD; the General Accounting Office; the Army Audit Agency; the Naval Audit Service; and the Air Force Audit Agency. We reviewed those reports and testimony for general and specific information about the questions set forth in the OMB reporting guidance.

We coordinated our evaluation efforts with DoD IT officials. However, we did not evaluate the methodology DoD used to select IT systems, evaluate its security posture, and develop its responses to the OMB questions.

4. Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law (Section 2534(a)(2) of the Security Act.)

Of the 49 reports summarized in the Information Assurance Challenges report, 23 DoD reports, about 45 percent (issued by the Office of the Inspector General, Army Audit Agency, Naval Audit Service, and Air Force Audit Agency), specifically stated that policies, procedures, or practices for information assurance were a management control weakness. See Appendix E

for a listing of those reports. Thirteen reports specified that the management control weaknesses identified were material. The following reports provide examples of identified material weaknesses:

Inspector General, DoD, Report No. D-2001-017, "Unclassified but Sensitive Internet Protocol Router Network Security Policy," December 12, 2000, provided an example of a material weakness in management controls. The Non-secure Internet Protocol Router Network (NIPRNet) is a network of Government-owned Internet protocol routers used to exchange unclassified but sensitive information among DoD users. The lack of security policy guidelines for the NIPRNet was a material management control weakness. The guidance that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued was outdated, unclear about the direct Internet connection waiver process, and not formal DoD policy. Consequently, the requirement to follow the guidance was unenforceable and DoD lacked effective management controls over Internet access. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) agreed to take corrective actions, which are ongoing.

The Air Force Audit Agency also reported control weaknesses on the NIPRNet. The weaknesses involving the NIPRNet, along with another information assurance weakness, resulted in the Air Force reporting the weaknesses in its FY 2000 Statement of Assurance. Corrective actions planned included fielding network protection and management tools, certified professionals, and techniques and procedures to monitor, manage and protect networks. See question 4, Appendix D, for details.

The Army Audit Agency reviewed documents about the material weakness in information security that the Army had reported since FY 1996. The Army statements of assurance reported deficiencies in systems and network security design and implementation; incident response, containment, and countermeasures; and information security education, training, and awareness. The Army's corrective action plan identified 32 corrective action milestones, of which 20 were complete by FY 2000. See question 4, Appendix C, for details.

The Naval Audit Service issued Report No. N2000-0045, "Navy Working Capital Fund Financial Management Feeder Systems for Fiscal Year 1999," September 29, 2000, which discussed material control weaknesses with the feeder systems to the working capital fund. The weaknesses included inadequate access controls, contingency planning, and system documentation. The Navy agreed to take corrective actions, which included an inventory of systems that provide financial data or support financial transactions in the Navy Working Capital Fund. The corrective actions were ongoing.

5. Succinctly describe the specific measures of performance used by the agency to ensure that agency program officials have: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and

4) tested and evaluated security controls and techniques. Include information on the actual performance for each of the four categories. (Section 3534(a)(2) of the Security Act.)

The DoD integrated the four categories listed into its DITSCAP program. Based on the results of our review of 90 applications from the subset of applications from DISA Centers, DoD had not fully implemented security policy. Written, current certification and accreditations were not available for an estimated 60 percent of the subset of 1,365 applications. Certification and accreditation are the technical evaluation of security features of an application or system and the formal declaration to operate the application or system. The DoD managers had not fully implemented information security policy because definitions for system, application, and other means of establishing security parameters and responsibilities were unclear. The parameters of and responsibility for information security were further obscured by the DoD practice of approving different organizations to design, develop, manage, use, and operate IT applications. In addition, the policy proponent, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); the service provider, DISA; and the Component heads provided limited oversight of policy implementation or policy applicability to the current IT environment.

In two reports, the Army Audit Agency recommended that the Army improve its process for measuring outcomes of information assurance investments. The Army subsequently developed 10 performance measures pertaining to information security. However, 6 of the 10 performance measures that the Army developed addressed only one of the categories from the OMB question: testing and evaluating security controls and techniques. None of the performance measures addressed the other OMB question categories of assessing risk, identifying appropriate security levels, or maintaining a current security plan. See question 5, Appendix C, for details.

The Air Force Audit Agency determined that managers for 76 percent of the 29 applications that it evaluated (19 applications as part of the Office of the Inspector General review and 10 supplemental applications) had not measured performance in any of the four information security categories. The Air Force managers labeled those systems that did not meet the criteria as legacy systems, which were systems that have operated for many years. The Air Force results for new and reengineered systems were more positive. According to results from Project No. 98066024, "Certification of Standard Systems," September 30, 1999, the Air Force effectively assessed risks, determined the proper level of security, maintained their security plan, and tested the security for new and reengineered systems. See question 5, Appendix D, for details.

6. Describe the specific measures of performance used by the agency to ensure that the agency CIO: 1) adequately maintains an agency-wide security program; 2) ensures the effective implementation of the program and evaluates the performance of major agency components; and 3) ensures the training of agency employees with significant security responsibilities.

Include information on the actual performance for each of the three categories. (Section 3534(a)(3)-(5) of the Security Act.)

Although DoD Directive 5200.28 specifically assigns oversight and review of implementation of its stated policies to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), the Assistant Secretary had not established a mechanism to provide that oversight. Additionally, Directive 5200.28 assigns responsibility to DoD Component heads for implementing and ensuring compliance with the endorsed policy and for programming funds and resources to support information security. The DoD Components also had no mechanisms for comprehensively measuring compliance with Directive 5200.28.

In a February 9, 2001, memorandum to all Components, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that DoD had several vehicles in place to assess information assurance and meet the intent of GISRA. According to the memorandum, the DoD required a means of evaluating and consolidating information assurance data to report the DoD information security posture. With the February memorandum, the Assistant Secretary established an integrated process team to accomplish that goal. The team developed only reporting criteria, methodology, and a report format for the FY 2001 DoD program reviews of unclassified systems; however, neither the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) nor the integrated process team established a security plan for DoD enterprise information that would consistently apply information security requirements to all DoD systems and networks. Further, the changing IT environment made maintaining current security policies and practices difficult.

7. Describe how the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training were available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training. (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act.)

We did not identify the total number of DoD employees who required information security training, the types of security training available during the reporting period, the number of DoD employees who received each type of training, or the total costs of providing training. In Inspector General, DoD, Report No. D-2001-182, "Information Assurance Challenges—a Summary of Results Reported April 1, 2000, through August 22, 2001," we observed that the DoD was progressing towards its information assurance training and certification requirements. DoD established the Human Resources Development Functional Area to develop and institute the means to continually improve education, training, and personnel awareness required to carry out the DoD information assurance mission.

The Information Assurance Challenges report also stated that DoD needs to further improve its information security training as evidenced by 11 reports that identified information security training vulnerabilities. For example, one report stated that the DoD needs to increase user awareness and understanding

regarding unusual and suspicious e-mail and other computer-related activities. Another report stated that to effectively deploy the public key infrastructure, DoD needs to train both users and system administrators to use complex and difficult technology.

The Army Audit Agency reported lack of training as a cause of systemic information security weaknesses in FY 1999 and FY 2000 audit reports. The Army Audit Agency followed up on those reports and identified Army actions to identify training needs for information security personnel over the last 2 years. The Army estimated that it had 14,000 information security personnel who required training. The Army budget was $2.9 million annually for information security training over the last 2 years. In FY 2000, the Army trained 6,650 information systems security personnel. The Army goal is to reach all information systems security personnel to provide the technical training necessary to protect information systems. See question 7, Appendix C, for details.

8. Describe the agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services Administration's FedCIRC. Include information on the actual performance and the number of incidents reported. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act.)

The results of prior audits and investigations showed that the DoD made progress in reporting and investigating security incidents, but additional improvements were needed. For example, Inspector General, DoD, Report No. D-2001-013, "DoD Compliance With the Information Assurance Vulnerability Alert Policy," December 1, 2000, evaluated DoD procedures for reporting security incidents and sharing information about common vulnerabilities. The report stated that DoD had made significant progress towards implementing its procedures and planned to be fully compliant by April 2001. However, as of August 31, 2001, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), had not issued a formal instruction, identified the positions and skills needed by the primary and secondary points of contact, or issued an implementation plan for the Information Assurance Vulnerability Alert process.

The Defense Criminal Investigative Service participates as a member of the Law Enforcement and Counterintelligence Center that DoD established to coordinate criminal and counterintelligence computer intrusion investigations and to disseminate relevant information to the military commands. The Defense Criminal Investigative Organizations (Army Criminal Investigation Command, Naval Criminal Investigative Service, Air Force Office of Special Investigations, and Defense Criminal Investigative Service) reported 86 incidents of root access and 313 incidents of other access for the period from October 1, 2000, through July 31, 2001. The Defense Criminal Investigative Organizations reported computer crime activity for that period of 194 investigations initiated, 178 investigations closed, 24 indictments, and 18 convictions. The total monetary recoveries and cost avoidance from computer crime investigations for that period amounted to $2.9 million.

Additionally, the Army Audit Agency issued two reports on procedures for reporting security incidents and sharing common vulnerabilities: Report No. AA 00-286, "Information Assurance—Phase IV: Reporting Process and Vulnerability Assessment Results," June 30, 2000, and Report No. AA 00-287, "Information Assurance—Phase V: Information Assurance Vulnerability Alert Process," June 30, 2000. The Army Audit Agency reported positive progress towards implementing security incident reporting procedures. According to the Army Audit Agency, the Army further improved its information security posture by establishing the Army Computer Emergency Response Team and the Information Assurance Vulnerability Alerts Compliance Verification Team. The Compliance Verification Team reports quarterly to the Secretary of the Army through the Office of the Director of Information Systems for Command Control, Communications, and Computers. The Army's Computer Emergency Response Team accomplished external reporting through the Joint Task Force—Computer Network Operations. The Joint Task Force communicated information to the Federal Computer Incident Response Capability and to external law enforcement. As of June 18, 2001, the Army reported 10,386 incidents. See question 8, Appendix C, for details.

9. Describe how the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY02 capital asset plan (as well as exhibit 53) submitted by the agency to OMB? If no, why not? (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

The Office of the Inspector General, DoD, cannot comment on whether DoD reported security requirements and costs on every FY 2002 capital asset plan or exhibit 53 that it submitted to OMB because time did not permit examination of those plans.

The Army Audit Agency reviewed some aspects of capital planning and investment that it reported in Report No. AA 01-284, "Workload Survey for Information Technology," May 31, 2001. The Army Audit Agency reported that the Army's Investment Strategy Working Group prioritized information technology investments and aligned the Army's portfolio of systems with its requirements. In its review of two Management Decision Packages for information assurance, the Army Audit Agency reported that the Army disseminated clear guidance on capturing security requirements. In addition, the Army appropriately identified the Management Decision Packages as its tool to capture information assurance requirements, report milestones, and specify costs (training, salaries, and tools). See question 9, Appendix C, for details.

10. Describe the specific methodology (for example, Project Matrix review) used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

We did not identify or review a specific DoD methodology to identify, prioritize, and protect critical assets within the DoD enterprise architecture.

However, the Inspector General, DoD, reported on improvements needed in related areas.

Mission or Business Area IT Investments. Inspector General, DoD, Report No. D-2001-175, "Application of Year 2000 Lessons Learned," August 22, 2001, stated that although the DoD CIO could have used the core processes, missions, and systems identified during the year 2000 effort to manage information technology investments, he had not. The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) implement a mission or business area approach for managing information technology investments. A mission or business area approach would necessitate identifying and prioritizing critical assets within the enterprise architecture.

Identification in the DoD IT Registry. The IT Registry is required by title VIII, subtitle B, "Information Technology," section 811, Public Law 106-398, which directs that all DoD Components must register, and thereby identify, mission-critical and mission-essential IT systems with the DoD CIO before the systems can be funded. As of August 30, 2001, DoD Components registered 3,783 unclassified mission-critical and mission-essential IT systems in the IT Registry. We compared our subset of systems from DISA Centers to the IT Registry. Not all systems operated on DISA platforms were registered. Of the 90 items that the Inspector General, DoD; the Army Audit Agency; and the Air Force Audit Agency sampled, 21 were also listed in the IT Registry. In addition, 10 applications in that sample supported 2 other major systems listed in the IT Registry. We did not review the effectiveness or completeness of the IT Registry.

The Army Audit Agency conducted a limited review of the Army's methodology and use of the IT Registry. The Army Audit Agency reported that the Army used the IT Registry to identify critical assets, including links with key external systems. According to the Army Audit Agency's August 2001 GISRA response, the Army had registered 1,090 mission-critical and mission-essential systems.

Contingency Planning. Inspector General, DoD, Report No. D-2001-182, "Information Assurance Challenges--A Summary of Results Reported April 1, 2000, through August 22, 2001," September 19, 2001, listed 11 reports that identified weaknesses in contingency planning. Contingency planning also requires identifying and prioritizing critical assets.

Certification and Accreditation. The DITSCAP establishes a standard certification and accreditation process for information technology that leads to more secure system operations and a more secure Defense information infrastructure. The certification and accreditation process should consider the system mission, environment, architecture, and impact on the Defense information infrastructure. The results of the Inspector General, DoD, review of DITSCAP implementation are discussed in question 11.

Programs to Protect Critical IT Assets—Not Evaluated. The DoD had several programs designed to protect IT assets. The programs did not require identification or prioritization within the enterprise architecture.

Defense in Depth. The DoD has an information assurance strategy called Defense in Depth, which the Office of the Inspector General, DoD, has not yet evaluated. The Defense in Depth strategy integrates the capabilities of people, operations, and technology to achieve strong, effective, multi-layer, multi-dimensional protection. That concept includes firewalls, external routers to filter unauthorized traffic, switches to process and filter authorized types of communications, and closing the vulnerabilities in each device connected to the network.

Joint Task Force—Computer Network Defense. The Joint Task Force—Computer Network Defense, which achieved initial operational capability in January 1999, has the goal of coordinating defense and detecting intrusion of DoD computer networks and systems. The Joint Task Force collects data on organized information attacks against critical DoD information networks, formulates courses of action against threat attacks, coordinates and directs DoD actions for defense, and prioritizes survey-action and mission-critical workarounds.

Law Enforcement and Counterintelligence Center. The Defense Criminal Investigative Service participates in the Law Enforcement and Counterintelligence Center. The Center investigates criminal and counterintelligence computer intrusions, coordinates its investigations with other law enforcement agencies, and disseminates information to the military commands to protect the security of military operations.

11. Describe the measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

We reviewed the implementation of the DITSCAP process as an objective for the subset of systems that we sampled. The DITSCAP, according to DoD Instruction 5200.40, applies to all life-cycle phases of DoD systems. We determined that an estimated 60 percent of the 1,365 applications from which we selected our sample did not have current certifications and accreditations, using the DITSCAP or any other assessment tool. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that it had several vehicles in place to assess information assurance but did not have a way to evaluate and consolidate information assurance data to report the DoD information security posture. Without the means of evaluating and consolidating data, DoD could not measure performance of information security throughout a system's life cycle.

12. Describe how the agency has integrated its information and information technology security program with its critical infrastructure protection

responsibilities, and other security programs (for example, physical and operational). (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act.)

The Office of the Inspector General, DoD, participated in the Joint Task Force—Computer Network Defense and the National Infrastructure Protection Center programs. Both programs contribute to the protection of critical infrastructure assets and information and are described below.

Joint Task Force—Computer Network Defense. In response to Presidential Decision Directive 63, "Critical Infrastructure Protection," May 1998, the DoD established a joint military organization to identify and mitigate threats to DoD information networks and direct the defense of the Defense Information Infrastructure. The mission of the U.S. Space Command, Joint Task Force—Computer Network Defense is to coordinate and direct the defense of DoD computer systems and information networks in conjunction with the unified commands, Services, and Defense agencies. In addition, Presidential Decision Directive 63 requires each Executive department to develop a plan and take deliberate actions to protect its specific information infrastructure.

National Infrastructure Protection Center. The National Infrastructure Protection Center, established in February 1998, coordinates investigative information related to computer network intrusions and provides early warnings of threats. It is an interagency, public-private entity of representatives from Federal agencies, including DoD, state and local governments, and the private sector. Presidential Decision Directive 63 requires that DoD assign personnel to the National Infrastructure Protection Center. DoD assigned 18 personnel for 2 years, with an option to extend for another year. The assigned positions ranged from administrative assistant to Deputy Chief, National Infrastructure Protection Center, and included criminal investigators in management positions.

Since May 2000, the General Accounting Office testified several times about critical infrastructure protection, including the DoD critical infrastructure. The testimony summarized that the DoD and others needed to improve efforts to protect critical infrastructure; specifically, efforts to gather and share data. For example, the Director of Governmentwide and Defense Information Systems and the Director of the Office of Computer Information Technology Assessment, General Accounting Office, testified in May 2000 about the ILOVEYOU computer virus. The testimony included DoD as an example of an entity requiring action because of the virus. DoD was also one of the subjects of critical infrastructure testimony in June, July, and September 2000, and May 2001.

13. Describe the specific methods (for example, audits or inspections) used by the agency to ensure that contractor-provided services (for example, network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB

policy and NIST guidance, national security policy, and agency policy. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

Audits are one method DoD uses to identify weaknesses in the policies and procedures used to acquire IT assets and services. In the past 2 years, six reports were issued addressing contractor developed and provided software.

Inspector General, DoD, Report No. D-2001-141, "Allegations to the Defense Hotline on the Defense Security Assistance Management System," June 19, 2001, stated that since 1995, the contractor for the Defense Security Assistance Management System used 174 employees without security investigations, including at least 38 foreign nationals, to work on the system. The report further stated that contractor employees without security investigations worked on 52 out of 364 task orders reviewed that were awarded on the DISA Defense Enterprise Integration Services II contract. Management agreed to amend DoD Regulation 5200.2-R to require uniform investigative and adjudicative requirements for all contractor employees including foreign nationals.

Inspector General, DoD, Report No. D-2001-127, "Data Reliability Assessment Review of win.COMPARE^2 Software," May 23, 2001, stated that the win.COMPARE^2 software, for which the Air Force contracted development, had adequate general and application controls.

Inspector General, DoD, Report No. D-2001-148, "Automated Transportation Payments," June 22, 2001, stated that the U.S. Transportation Command contracted for a commercial electronic commerce package to make transportation payments. The commercial package did not have adequate controls to safeguard sensitive financial information or ensure production of reliable data. In addition to recommendations on the specific commercial package, the report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) clarify and expand the guidance on commercial products.

The Air Force Audit Agency completed three audits on contractor-provided services: Report No. 99066040, "Air Force Research Laboratory UNIX-Based Computer Systems," May 21, 2001; Report No. 99066017, "Information Assurance—Implementing Controls Over Known Vulnerabilities in Air Force Space Command Computers," May 26, 2000; and Report No. 99066019, "Information Assurance—Implementing Controls Over Known Vulnerabilities in Air Force Materiel Command Computers," March 2, 2000. The Air Force contract administration efforts and oversight provisions did not provide adequate managerial control. Specifically, contracts within two major commands did not specify performance criteria for implementing countermeasures identified in the Air Force Computer Emergency Response Team advisories. All five contracts reviewed at one major command did not contain requirements for the contractor to adhere and respond to the advisories in required time frames. During followup within that command, the Air Force Audit Agency noted that the command leadership began reversing contracting-out efforts and turning to military and civil service personnel for operating networks and technology services for the command.

Appendix A. Evaluation Process

Scope

This report is in response to the GISRA requirements of the Floyd D. Spence National Defense Authorization Act for FY 2001. This report includes information assurance weaknesses identified in the Information Assurance Challenges summary report, which discussed reports issued from April 1, 2000, through August 22, 2001, and results from the independent evaluation of a subset of DoD systems. The independent evaluation, Inspector General, DoD, Report No. D-2001-183, "Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers," September 19, 2001, was accomplished January through July 2001. The Army Audit Agency and Air Force Audit Agency supported the GISRA effort by evaluating applications in the selected subset and by responding to the OMB questions in Memorandum 01-24, "Reporting Instructions for the Government Information Security Reform Act."

DoD-Wide Corporate Level Government Performance and Results Act Coverage. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to information assurance as well as achievement of the following goal, subordinate performance goal, and performance measure.

- **FY 2001 DoD Corporate Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-02)**

- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-DoD-2.5) FY2001 Performance Measure 2.5.3:** Qualitative Assessment of Reforming Information Technology (IT) Management. **(01-DoD-2.5.3)**.

Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

Information Management Functional Area.

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate Defense Information Infrastructure. **(IM-2.3) Goal:** Improve information technology management tool. **(IM-2.5)**

- **Objective:** Reform information technology management processes to increase efficiency and mission contribution. **Goal:** Institutionalize provisions of the Information Technology Management Reform Act of 1996. **(IM-3.1) Goal:** Institute fundamental information technology management reform efforts. **(IM-3.2)**

- **Objective:** Ensure DoD's vital resources are secure and protected. **Goal:** Make Information Assurance (IA) an integral part of DoD Mission Readiness Criteria. **(IM-4.1)**

General Accounting Office High-Risk Area. The General Accounting Office lists information assurance as a high-risk area. Although the Secretary of Defense annually establishes DoD-wide corporate-level goals and performance measures to address the requirements of the Government Performance and Results Act, the Department does not currently provide corporate-level goals for information assurance. This report provides coverage of the Information Security and System Modernization high-risk areas.

Methodology

To assess the IT security posture of DoD, we selected a random sample of applications from a subset of systems. For those applications, the objective was to identify security personnel, such as the information system security officer and the designated approval authority, and to determine whether the applications had a Certification and Accreditation or an Interim Authority to Operate. We constructed a spreadsheet in which to compile and analyze results from our subset of systems.

Use of Computer-Processed Data. Computer-generated information was the source for selecting the subset, but was not used as evidence in a finding.

Universe and Sample. We identified applications operating or residing on the DISA Centers and Detachments as our subset of systems, the universe for this sample. In response to our request for DISA-supported applications, DISA Western Hemisphere provided a listing of 4,939 applications on Center and Detachment systems that were billed to customers. We did not validate the number of applications that DISA provided on its listing. Analysis of the 4,939 applications determined that multiple occurrences of the same names appeared. Operations research analysts from the Quantitative Methods Division, Office of the Assistant Inspector General for Auditing, aggregated the list to include only unique names of applications, which left 1,365 applications. The analysts then generated a simple random sample of 90 applications.

Measurement Issues. The listing of applications that DISA Western Hemisphere provided consisted of every line item billed by DISA. Some items were not, in fact, applications, but space on the network that customers must pay to use. We also found inactive or unacknowledged applications, so we could not test the sample items for the attributes demonstrating security policy implementation. See Appendix C for details of the 90 sample applications. The

categories of sample results and the number of applications in each category are shown below.

Table A1. Sample Results by Certification and Accreditation Status Category

Category	Sample Result
Current Certification and Accreditation or Interim Authority to Operate	33
Out of Date Certification and Accreditation or Interim Authority to Operate	2
No Certification and Accreditation and no Interim Authority to Operate, or incomplete	19
Other IT	9
Unable to test the Certification and Accreditation or Interim Authority to Operate status	27
Total	**90**

Measurement Results. The operations research analysts projected the confidence intervals reported below using a 90 percent confidence level. The results shown in the report are the point estimates projected for the universe of 1,365 unique applications. The complete results of the projections are shown below.

Table A2. Certification and Accreditation Status Projected to the Population of Applications

Category	Lower Bound	Point[1] Estimate	Upper Bound
Current Certification and Accreditation or Interim Authority to Operate	383	501	618
Out of date Certification and Accreditation or Interim Authority to Operate	--[2]	30	72
No Certification and Accreditation and no Interim Authority to Operate, or incomplete (certification only)	187	288	389
Other IT	60	137	213
Unable to test the status of the Certification and Accreditation or Interim Authority to Operate	297	410	522

[1]The point estimate does not add up to the population due to rounding.
[2]The lower bound estimate is below zero; therefore, it is not reported.

Use of Audit Assistance. The Army Audit Agency and the Air Force Audit Agency gathered and analyzed data for those sample items that belonged to customers within their respective Component. The Army Audit Agency gathered and analyzed data for 34 sample items, and the Air Force Audit Agency gathered and analyzed data for 19 sample items. We accepted that data without further review and merged it into a common spreadsheet for interpretation of the overall sample results. The Army Audit Agency and the Air Force Audit Agency also provided responses to the specific questions from the OMB reporting guidance. See Appendixes C and D, respectively.

Use of Technical Assistance. One computer engineer from the Technical Assessment Division, Office of the Assistant Inspector General for Auditing, assisted in planning the audit. In addition, two operations research analysts from the Quantitative Methods Division, Office of the Assistant Inspector General for Auditing, assisted in selecting the random sample from the subset of applications and interpreting the results.

Evaluation Dates. We conducted this program evaluation from January 2001 through August 2001, in accordance with standards issued by the Inspector General, DoD. The reports that provided source information were issued between April 1, 2000, and August 22, 2001.

Contacts During the Audit. We visited or contacted individuals and organizations within the DoD. Further details are available upon request.

Appendix B. Prior Coverage

The following reports discussing elements of information security in the DoD were issued from April 2000 through August 2001. Summaries of each of the listed reports appear in Report No. D-2001-182, "Information Assurance Challenges--a Summary of Results Reported April 1, 2000, through August 22, 2001," September 19, 2001

General Accounting Office

GAO-01-959T, "Electronic Government: Challenges Must be Addressed with Effective Leadership and Management," July 11, 2001

GAO-01-783, "Department of Defense: Status of Achieving Outcomes and Addressing Major Management Challenges," June 25, 2001

GAO-01-769T, "Critical Infrastructure Protection—Significant Challenges in Developing Analysis, Warning, and Response Capabilities," May 22, 2001

GAO-01-600T, "Computer Security—Weaknesses Continue to Place Critical Federal Operations and Assets at Risk," April 5, 2001

GAO-01-583T, "Information and Technology Management—Achieving Sustained and Focused Governmentwide Leadership," April 3, 2001

GAO-01-307, "Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program," March 30, 2001

GAO-01-341, "Information Security: Challenges to Improving DoD's Incident Responsibilities Capabilities," March 29, 2001

GAO-01-277, "Information Security—Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology," February 26, 2001

GAO-01-89, "Financial Management: Significant Weaknesses in Corps of Engineers' Computer Controls," October 11, 2000

GAO/T-AIMD-00-314, "Computer Security—Critical Federal Operations and Assets Remain at Risk," September 11, 2000

GAO/AIMD-00-296R, "Federal Agencies' Fair Information Practices," September 11, 2000

GAO/AIMD-00-295, "Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies," September 6, 2000

GAO/T-AIMD-00-268, "Critical Infrastructure Protection—Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination," July 26, 2000

GAO/AIMD-00-188R, "Software Change Controls at the Department of Defense," June 30, 2000

GAO/T-AIMD-00-229, "Critical Infrastructure Protection—Comments on the Proposed Cyber Security Information Act of 2000," June 22, 2000

GAO/AIMD-00-209R, "Defense Software Development," June 15, 2000

GAO/T-AIMD/GGD-00-179, "Electronic Government—Federal Initiatives Are Evolving Rapidly But They Face Significant Challenges," May 22, 2000

GAO/T-AIMD-00-181, "Critical Infrastructure Protection—"ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities," May 18, 2000

GAO/T-AIMD-00-171, "Information Security—"ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements," May 10, 2000

Inspector General, DoD

Report No. D-2001-183, "Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers," September 19, 2001

Report No. D-2001-182, "Information Assurance Challenges-A Summary of Results Reported April 1, 2000, through August 22, 2001," September 19, 2001

Report No. D-2001-175, "Application of Year 2000 Lessons Learned," August 22, 2001

Report No. D-2001-166, "Defense Joint Military Pay System Security Functions at Defense Finance and Accounting Service Denver," August 3, 2001

Report No. D-2001-148, "Automated Transportation Payments," June 22, 2001

Report No. D-2001-141, "Allegations to the Defense Hotline on the Defense Security Assistance Management System," June 19, 2001

Report No. D-2001-137, "Certification of the Defense Civilian Personnel Data System," June 7, 2001

Report No. D-2001-136, "Defense Clearance and Investigations Index Database," June 7, 2001

Report No. D-2001-130, "DoD Internet Practices and Policies," May 31, 2001

Report No. D-2001-127, "Data Reliability Assessment Review of win.COMPARE^2 Software," May 23, 2001

Report No. D-2001-101, "Controls Over Electronic Document Management," April 16, 2001

Report No. D-2001-095, "Controls for the Electronic Data Interchange at the Defense Finance and Accounting Service Columbus," April 6, 2001

Report No. D-2001-068, "Inspector General, DoD, Oversight of the Audit of the FY 2000 Military Retirement Fund Financial Statements," February 28, 2001

Report No. D-2001-055, "General Controls for the Defense Civilian Pay System," February 21, 2001 (For Official Use Only)

Report No. D-2001-052, "Controls Over the Defense Joint Military Pay System," February 15, 2001 (For Official Use Only)

Report No. D-2001-044, "Accreditation Policies and Information Technology Controls at the Defense Enterprise Computing Center Mechanicsburg," February 9, 2001 (For Official Use Only)

Report No. D-2001-046, "Information Assurance at Central Design Activities," February 7, 2001

Report No. D-2001-029, "General Controls Over the Electronic Document Access System," December 27, 2000

Report No. D-2001-019, "Program Management of the Defense Security Service Case Control Management System," December 15, 2000

Report No. D-2001-017, "Unclassified but Sensitive Internet Protocol Router Network Security Policy," December 12, 2000

Report No. D-2001-016, "Security Controls Over Contractor Support for Year 2000 Renovation," December 12, 2000

Report No. D-2001-013, "DoD Compliance with the Information Assurance Vulnerability Alert Policy," December 1, 2000

Report No. D-2000-182, "Data Processing Control Issues for the FY 1999 Military Retirement Fund," August 31, 2000 (For Official Use Only)

Report No. D-2000-142, "Defense Information Systems Agency's Acquisition Management of the Global Combat Support System," June 9, 2000

Report No. D-2000-139, "Controls Over the Integrated Accounts Payable System," June 5, 2000

Report No. D-2000-122, "Information Assurance in the Advanced Logistics Program," May 12, 2000

Report No. D-2000-116, "Configuration Changes to Year 2000 Compliant Mission-Critical and Date-Dependent Systems," April 25, 2000

Army

Report No. AA 01-319, "Corps of Engineers Financial Management System: General and Application Controls," June 26, 2001

Report No. AA 00-287, "Information Assurance—Phase V: Information Assurance Vulnerability Alert Process," June 30, 2000

Report No. AA 00-286, "Information Assurance—Phase IV: Reporting Process and Vulnerability Assessment Results." June 30, 2000 (For Official Use Only)

Navy

Report No. N2001-0029, "Department of the Navy Principal Statements for FY 2000: Feeder Systems and Interfaces," June 1, 2001

Report No. N2000-0045, "Navy Working Capital Fund Financial Management Feeder Systems for Fiscal Year 1999," September 29, 2000

Air Force

Report No. 01066018, "Access Controls at Air Force High Performance Computing Centers," June 26, 2001

Report No. 01066002, "Database Security Controls," June 7, 2001

Report No. 99066040, "Air Force Research Laboratory UNIX-Based Computer Systems," May 21, 2001

Report No. 00054006, "Air Force Restoration Information Management System Controls," May 18, 2001

Report No. 00066006, "Implementation of Network Management System/Base Information Protection," May 1, 2001

Report No. 99066041, "Controls Over Air Force Composite Health Care Systems," December 13, 2000

Report No. 99066038, "Web Page Management," November 8, 2000 (For Official Use Only)

Report No. 99054027, "Review of Controls in the Command Online Accounting and Reporting System (COARS)," November 1, 2000

Report No. 99066018, "Information Assurance—Implementing Controls Over Known Vulnerabilities in Pacific Air Force Computer Systems," August 11, 2000 (For Official Use Only)

Report No. 99066024, "Information Assurance—Implementing Controls Over Known Vulnerabilities in Air Force Reserve Command Computers," July 7, 2000 (For Official Use Only)

Report No. 99066017, "Information Assurance—Implementing Controls Over Known Vulnerabilities in Air Force Space Command Computers," May 26, 2000 (For Official Use Only)

Report No. 99066028, "Controls Within the Acquisition Due-In System," May 1, 2000

Appendix C. Army Audit Agency Response to OMB Questions

INTRODUCTION

The Government Information Security Reform Act, passed as part of the FY 01 Defense Authorization Act (Public Law 106-398), amended the Paperwork Reduction Act of 1995 by adding a new subchapter on information security. The Act codified existing security policies contained in Office of Management and Budget, Circular A-130, Appendix III. It reiterated security responsibilities outlined in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996. The Government Information Security Reform Act also added a requirement for annual agency program reviews and annual independent evaluations for both unclassified and national security programs.

Office of Management and Budget Memorandums 01-08 (16 January 2001) and 01-24 (22 June 2001) provided instructions to Agency Inspectors General. In the instructions, the office requested that the Inspectors General respond to 12 of the 14 specific questions listed in Memorandum 01-24, and to base their responses solely on the results of independent evaluations related to those questions. We conducted the Army's portion of the independent evaluation for the Department of Defense Inspector General's Office. The Defense-wide report will be provided to Congress for review.

QUESTIONS AND RESULTS

The Office of Management and Budget requested Inspectors' General input on Questions 2-13 from Office of Management and Budget Memorandum 01-24. Here are those questions and our results:

Question 2: Identify the total number of programs included in the program reviews or independent evaluations.

Results: The major components of the Army's agencywide security program are:

- Network Security Improvement Program (sustaining base).
- Information Assurance Training Program.
- Training Tactical Information Assurance Program (tactical).

- Communication Security Program.
- Key Management Infrastructure.
- Public Key Infrastructure Program.
- Accreditation and Certification Program.
- Policy Development, Coordination, and Promulgation.
- Biometrics Program.
- Application Security Program.

We didn't perform an entire review of the Army's agencywide security program; however, we have looked at several of the security initiatives.

Question 3: Describe the methodology used in the program reviews and the methodology used in the independent evaluations.

Results: We relied on the following prior audit reports to accomplish this initial reporting requirement for the Government Information Security Reform Act:

Title of Audit Report	Audit Report Number
Performance Measures for Information Systems Security	AA 97-767
Information Systems Security Program Phase II Follow-On Validation	AA 99-005
Information Assurance--Phase III: Funding and Performance Measures	AA 00-001
Audit Of Mission Critical Systems Y2K	AA 00-012
Information Assurance--Phase IV: Reporting Process and Vulnerability Assessment Results	AA 00-286
Information Assurance--Phase V: Information Assurance Vulnerability Alert Process	AA 00-287
Workload Survey Report for the Army's Long Range Corporate Information Technology Audit Plan	AA 01-284

These audits were performed, in most material respects, in accordance with generally accepted auditing standards. We also performed a limited review to update our prior audit results.

Question 4: Report any material weakness in policy, procedures, or practices as identified and required to be reported under existing law (Section 3534(c)(1)-(2) of the Government Information Security Reform Act).

Results: The Army identified and reported Information Security as a material weakness in FY 96. We reviewed the Army's Uncorrected Material Weakness documents from FY 96 through FY 00 and found that there was widespread recognition that the Army's unclassified automated information systems and telecommunications networks have been attacked and successfully penetrated by unauthorized personnel. These intrusions led to the identification of systematic deficiencies in systems and network security design and implementation. To correct these weaknesses, Army leadership developed the Command and Control Protect Program Management Plan and outlined the measures needed to ensure that the Army's portion of the Defense Information Infrastructure was adequately protected. The Uncorrected Material Weakness documents we reviewed showed that the Army had planned 32 major milestones in corrective action and had completed 20 (62.5 percent) of these from FY 96 to FY 00.

Question 5: Succinctly describe the specific measures of performance used by the agency to ensure that agency program officials have: (1) assessed the risk to operations and assets under their control, (2) determined the level of security appropriate to protect such operations and assets, (3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control, and (4) tested and evaluated security controls and techniques. Include information on the actual performance for each of the four categories (Section 3534(a)(2) of the Government Information Security Reform Act).

Results: We issued two prior audit reports involving the Army's Information Security performance measures (Audit Reports AA 97-767 and AA 00-001). In these reports, we found that the

Army didn't have an effective process to objectively measure outcomes of Information Assurance investment initiatives and organizational changes made to enhance the operational readiness of the warfighter's sustaining base systems and networks. Since our reports were issued, the Army developed 10 performance measures pertaining to information security. However, none of the 10 performance measures were related to:

- Assessing the risk to operations and assets under the Army's control.
- Determining the level of security appropriate to protect operations and assets.
- Maintaining an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under the Army's control.

The Army had developed six performance measures that related to testing and evaluating security controls and techniques:

- Army Circuits Protected.
- Incidents Detected and Blocked.
- Intrusion Detected.
- Zone Transfers Detected and Denied.
- Domain Name Server Queries Denied.
- Information Assurance and Vulnerability Assessment Verification.

Question 6: Succinctly describe the specific measures of performance used by the agency to ensure that the agency Chief Information Officer (1) adequately maintains an agencywide security program, (2) ensures the effective implementation of the program and evaluates the performance of major agency components, and (3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories (Section 3534(a)(3)-(5) of the Government Information Security Reform Act).

Results: Performance measures weren't in place that measured how the Army Chief Information Officer maintained an agencywide security program, how he ensured the effective implementation of the program, or how he evaluated the performance of major agency components. Four performance measures were developed to help ensure that Army employees with significant security responsibilities were trained:

- Number of System Administrators Trained.
- Number of Information Assurance Managers Trained.
- Number of Defense Information Technology Security Certification and Accreditation Process Students Trained.
- Number of Information Assurance Workshop Students Trained.

However, other than the six performance measures we identified in our response to Question 5 on testing and evaluating security controls and techniques, performance measures hadn't been developed for the other major components of the Army's agencywide security program (identified in our conclusions to Question 2).

Question 7: Succinctly describe how the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training was available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Government Information Security Reform Act).

Results: Our prior audit reports (AA 99-005 and AA 00-001) identified that a main cause of systemic security problems within the Army was that the Army hadn't clearly identified training needs for information systems security personnel and that the training programs generally didn't:

- Reach all information systems security personnel.
- Provide the technical training necessary to protect information systems from unauthorized access, malicious attacks, exploitation, and denial of service.

The Army hadn't clearly identified the total number of security personnel in the Army. The Army estimated the number at about 14,000—including Information Assurance Program Managers, Information Assurance Managers, and System Administrators. Since our prior audits, the Army had implemented an aggressive training program over the last 2 years. The following table shows the courses offered and the enrollment data for FY 00:

Course	Enrollment
Information Assurance Manager Course	738
System Administration Course	4,212
Information Assurance Workshops	625
Defense Information Technology Security Certification and Accreditation Process Workshops	600
Defense Information Technology Security Certification and Accreditation Process Information Assurance Manager Course	475
Total Enrolled	6,650

The Information Assurance Training budget for the last 2 years has been $2.9 million annually. This excluded funds spent on training at the MACOM and installation levels, and the travel costs associated with attending classes at Fort Gordon.

Question 8: Succinctly describe the agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Computer Incident Response Capability. Include information on the actual performance and the number of incidents reported (Section 3534(b)(2)(F)(i)-(iii) of the Government Information Security Reform Act).

Results: Two prior audit reports (AA 00-286 and AA 00-287) addressed Army procedures for reporting security incidents. We audited the process, procedures, and controls used to ensure organizations effectively implemented the various components of "Positive Control" and compliance with Army Information Assurance Vulnerability Alert messages. The reports stated that the Army made significant improvements in its procedures to identify, report,

and respond to cyber intrusions and attacks. The Army further enhanced its Information Assurance posture by installing new network intrusion detection systems and establishing more effective monitoring and reporting capabilities. We did find, however, that reporting procedures related to the simulated attacks could be strengthened. Since then, the Army has continued to improve its Information Assurance posture. The Army Computer Emergency Response Team that specifically handles security issues was established. The team established a website that maintains all policies (for example, DOD and Army) related to Information technology, security, and system management. The site was updated as new policies were added.

Information Assurance Vulnerability Alerts were also maintained on a website. The page contained alerts, bulletins, and tech tips regarding various vulnerabilities. When a message or alert was received and the patch wasn't implemented, a report of the projected date of compliance was sent to Army Computer Emergency Response Team. Fixes had to be implemented no later than the timelines outlined in the messages. The website was the main channel for sharing vulnerability information with other agencies. The Army had also established an Information Assurance Vulnerability Alerts Compliance Verification Team. It was this team's responsibility to scan portions of the network for known vulnerabilities to check if they had been implemented. Any vulnerability found by the verification team was reported to the organization, and the organization was given 10 days to fix the vulnerability and report compliance. The organization was required to reply to the Director of Information Systems for Command, Control, Communications, and Computers stating what actions it had taken.

The Office of the Director of Information Systems for Command, Control, Communications, and Computers provided a quarterly status report of corrective actions to the Secretary of the Army. This report served to check the adequacy of the Army's "Positive Control" procedures. External reporting was handled through the Joint Task Force – Computer Network Operations. The Army Computer Emergency Response Team reported directly to the Joint Task Force who disseminated any information to the Federal Computer Incident Response Capability and external law enforcement.

As of 18 June 2001, 10,386 incidents had occurred.

Question 9: Succinctly describe how the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY 02 capital asset plan (as well as exhibit 53) submitted by the agency to Office of Management and Budget? If no, why not?
(Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6), and 3534(a)(C) of the Government Information Security Reform Act).

Results: We addressed some aspects of capital planning and investment control process in our Workload Survey Report (AA 01-284) for the Army's Long Range Corporate Information Technology Audit Plan. The Army had an Investment Strategy Working Group in place that provided a holistic approach for the Army to prioritize information technology investment solutions and align the Army's portfolio of Command, Control, Communications, Computers and Intelligence/Information Technology systems with Armywide requirements. It used four guiding principles:

- Link operational and institutional support investments with DOD and Army strategic mission goals.
- Balance resources between the warfighter and the institutional support base.
- Identify critical investments that provide the highest return on investments (value per dollar).
- Provide a framework for sound programming decisions.

During our review, we identified five Management Decision Packages associated with Information Assurance. Our review focused on the investment area "Information Assurance" and two Management Decision Packages: MS4X—Computer Security and MX5T—Information Systems Security. We found that the Army:

- Disseminated clear guidance on how to capture security requirements.
- Identified which Management Decision Packages to use for capturing Information Assurance requirements.
- Identified reporting milestones.
- Identified specific costs (training, salaries, and tools).

Question 10: Succinctly describe the specific methodology (for example, Project Matrix review) used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6), and 3534(a)(C) of the Government Information Security Reform Act).

Results: In our Summary of Year 2000 Audit Coverage – Lessons Learned (AA 00-214), we found that system managers, owners, and users didn't always have adequate configuration management controls for identifying and validating system configurations or architectures for mission-critical systems. We then conducted a limited review to determine how the Army currently identifies, prioritizes, and protects its mission-critical assets.

- Identify: The definition for a mission-critical information system, as defined in the Clinger-Cohen Act, is an information system and a national security system that would cause the stoppage of warfighter operations or direct mission support of warfighter operations if it were lost. Currently the Army uses the Information Technology (IT) registry to identify critical assets, including links with key external systems. The registry shows that there are 1,090 mission critical and mission essential systems for the Army.

- Prioritize: There is no Armywide standard or guidance on how the Army should prioritize its critical assets.

- Protect: Army Regulation 25-1 states that the Army should have the following security implemented in order to protect all information systems:

    - Physical Security.
    - Software Security.
    - Hardware Security.
    - Procedural Security.
    - Personnel Security.
    - Communications Security.

DA Information Assurance personnel expanded the list to include four additional topics of importance:

- o Domain Name Server.
- o Top Level Architecture.
- o Monitoring of the Top Level Architecture.
- o System Administrator and Network Manager Training.

Question 11: Succinctly describe the measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Government Information Security Reform Act).

Results: There were no performance measures used by the Army to ensure that its information security plan was practiced throughout the life cycle for each system supporting the operations and assets under its control. The Army Information System Security Program implemented prior Office of Management and Budget guidance and required all systems to be certified and accredited using a system security plan. However, no formal performance measures were identified to ensure that the guidance had been implemented. The Army did capture, on a monthly basis, the number of Non-Classified Internet Protocol Router Network circuits that had been accredited.

Question 12: Succinctly describe how the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (for example, physical and operational). (Sections 3534 (a)(1)(B) and (b)(1) of the Government Information Security Reform Act.)

Results: We haven't performed any audits that covered critical infrastructure protection responsibilities and, therefore, can't provide any results relative to this question.

Question 13: Succinctly describe the specific methods (for example, audits or inspections) used by the agency to ensure that contractor-provided services (for example, network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, Office of Management and Budget policy and the National Institute of Standards and Technology guidance, national security policy, and agency policy (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Government Information Security Reform Act).

Results: : We haven't performed any audits that covered critical infrastructure protection responsibilities and, therefore, can't provide any results relative to this question.

Appendix D. Air Force Audit Agency Response to OMB Questions

OMB Questions to Answer

1. Identify the agency's total security funding as found in the agency's FY01 budget request, FY01 budget enacted, and the FY02 budget request. This should include a breakdown of security costs by each major operating division or bureau and include critical infrastructure protection costs that apply to the protection of government operations and assets.[1] Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public[2].

Response: No response needed.

2. Identify the total number of programs included in the program reviews or independent evaluations.

Response: During this cycle of our independent evaluations, we evaluated the certification and accreditation of a random sample of 29 systems from a universe of 105 systems identified by the DoD Inspector General.

3. Describe the methodology used in the program reviews and the methodology used in the independent evaluations.

Response: Within the independent evaluation, we determined whether the owners of the systems evaluated the threats to their system, identified the vulnerabilities within their system, took measures to mitigate the vulnerabilities, and reported the residual risk to the Designated Approving Authority. We also determined if that Designated Approving Authority formally approved the system to operate, given the identified level of residual risk.

4. Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law. (Section 3534(c)(1)-(2) of the Security Act).

[1] Agencies should report security costs which agree with those reported on their FY02 Exhibit 53. If security costs detailed in an agency's Exhibit 53 were incomplete or inaccurate, corrected security costs should be reported, and differences with the final FY02 Exhibit 53 noted.

[2] The following agencies have lead agency responsibilities pertaining to critical infrastructure protection: Commerce, Treasury, EPA, Transportation, FEMA, HHS, Energy, Justice, State, DOD, and CIA.

Response: In response to multiple Air Force Audit Agency Reports of Audit, the Air Force identified two information assurance-related material weaknesses in its FY 2000 Statement of Assurance. The first weakness was inadequate identification and correction of vulnerabilities within networked computers and lack of proper authorization before placing material on web servers. The second weakness was inadequate controls to preclude transmitting sensitive but unclassified information over the NIPRNET (Non-Secure Internet Protocol Router Network) that is not protected (e.g., encrypted) during transmission. Our independent evaluations indicate these material weaknesses continue to exist.

B. Security Program Performance

In this section, the agency shall succinctly describe:

5. The specific measures of performance used by the agency to ensure that agency program officials have: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques. Include information on the actual performance for each of the four categories. (Section 3534(a)(2) of the Security Act).

Response: In our FY 2001 evaluation of Certification and Accreditation of Air Force Systems, we determined that owners of 22 of 29 Air Force systems (76 percent) had not: 1) assessed the risk that operating their system posed to their operations and the operations of other systems on the networks; 2) determined the level of security appropriate to protect their operations and assets; 3) maintained an up-to-date security plan for their systems; or 4) tested and evaluated their system's security controls and techniques. Most systems reviewed were considered legacy systems that were operating for many years. On the contrary, for new and reengineered systems, another audit, Certification of Standard Systems (Project 98066024, 30 September 1999), indicated the Air Force was effectively assessing risks, determining the proper level of security, maintaining their security plan, and testing the security for those systems.

6. The specific measures of performance used by the agency to ensure that the agency CIO: 1) adequately maintains an agency-wide security program; 2) ensures the effective

implementation of the program and evaluates the performance of major agency components; and 3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories. (Section 3534(a)(3)-(5) of the Security Act).

Response: Although we are not aware of any specific "measures of performance" the Air Force users to evaluate its information assurance program, we provide the following comments:

1) The Air Force maintains an information security program complete with policies, directives, and common practices.

2) The prior Secretary of the Air Force and the Air Force CIO ensured the effective implementation of the information security program through quarterly briefings on information security-related issues including network security, base information protection, implementation of firewalls and pubic key encryption, etc. Further, the former Secretary tasked his internal auditors and the Air Force Inspector General to provide a number of evaluations of information security within the Air Force to include how well each major command was securing its networks. We assume the new Secretary will continue these practices.

3) Training security professionals has not been a topic for our review to date. However, we have coordinated with the HQ AF/SC staff and plan to evaluate the training of information assurance professionals within the Air Force in FY 2002.

7. How the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training was available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training. (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act).

Response: As indicated in our response to Item 6, sub-item 3, we have not completed audit work related to information assurance training, but we have an audit planned for FY 2002.

8. The agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services

Administration's FedCIRC. Include information on the actual performance and the number of incidents reported. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act).

Response: We have not performed audit work related to reporting security incidents and sharing the information regarding common vulnerabilities. We have an audit planned to address these issues in FY 2002.

9. How the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY02 capital asset plan (as well as exhibit 53) submitted by the agency to OMB? If no, why not? (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

Response: We have not completed audit work evaluating how the Air Force integrates security into its capital planning and investment control process. We do not have an audit scheduled on this area in the next 18 months.

10. The specific methodology (e.g., Project Matrix review) used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

Response: Using a concept of Defense in Depth, the Air Force protects its assets (networks, hardware, software, and information). That concept provides a layered approach that includes firewalls, external routers to filter unauthorized traffic, switches to process and filter authorized types of communications, and closing the vulnerabilities in each device (computer, printer, and router) connected to the network. Further, the 'sensitive but unclassified' resources ride along the Non-Secure Internet Protocol Router Network (NIPRNET), which affords the least protection. However, information classified at the 'Secret' level is transmitted over secure lines (Secret Internet Protocol Router Network – SIPRNET). Within the NIPRNET and SIPRNET, however, we know of no methodology for identifying and prioritizing the assets to be protected within the enterprise architecture.

11. The measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

Response: The Air Force Deputy CIO and his staff receive metrics on the status of information security within the Air Force. The former Deputy CIO briefed the forme Secretary of the Air Force quarterly on information assurance metrics and issues. Additionally, the former Secretary actively engaged both his internal auditors and inspector general to perform numerous audits and inspections evaluating how well the Air Force's information security policies were implemented. For the period 1998 to th present, AFAA completed 24 audits (see attached listing) addressing various informatic security-related issues. Although we cannot confirm, we assume the new Secretary of t Air Force will continue this level of oversight.

12. How the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., physical and operational). (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act).

Response: We have not completed audit work to evaluate integrating the information and information technology security programs to protect the critical infrastructure. We do not have an audit scheduled for this area for the next 18 months.

13. The specific methods (e.g., audits or inspections) used by the agency to ensure that contractor-provided services (e.g., network or website operations) or services provided l another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act).

Response: We completed three audits on this issue in the past 2 years. Audit work indicated contract administration efforts and oversight provisions in those contra did not provide adequate managerial control. Specifically, contracts within two major commands did not include specific performance criteria related to implementing countermeasures identified in the Air Force Computer Emergency Response Team advisories. For example, all five contracts reviewed in one major command did not contain requirements for the contractor to adhere and respond to the Air Force Computer Emergency Response Team advisories in the Air Force-required timeframes. During follow-up audit work within that command, we noted the command leadership began reversing their contracting-out efforts and turned more to military and civil

service personnel for operating the command's networks and technology services. This audit perspective is provided based on work at only two of the nine major commands in the Air Force and one research laboratory.

C. Next Steps

14. Each agency head, working with the CIO and program officials, must provide the following information to OMB by October 31, 2001. Provide a strategy to correct security weaknesses identified through the annual program reviews, independent evaluations, other reviews or audits performed throughout the reporting period, and uncompleted actions identified prior to the reporting period. Include a plan of action with milestones that include completion dates that: 1) describes how the agency plans to address any issues/weaknesses; and 2) identifies obstacles to address known weaknesses.

Response: No response needed.

Appendix E. Reports Specifying Management Control Weaknesses

DoD Reports (Inspector General, Army Audit Agency, Naval Audit Service, and Air Force Audit Agency) identified the following weaknesses in policies, procedures, or practices; the first 13 reports state that the weaknesses were material:

1. Inspector General, DoD, Report No. D-2001-148, "Automated Transportation Payments," June 22, 2001, stated that management controls over the automated transportation payment process were not adequate to ensure that DoD resources were safeguarded. The controls were not adequate to safeguard sensitive information or to ensure the production of reliable data.

2. Inspector General, DoD, Report No. D-2001-055, "General Controls for the Defense Civilian Pay System," February 21, 2001, identified multiple weaknesses. The report discussed establishing an overall security program, controlling access to the system, implementing procedures for developing and changing computer software, establishing policies for proper segregation of duties, and establishing procedures for preventing disruptions in service to customers.

3. Inspector General, DoD, Report No. D-2001-052, "Controls Over the Defense Joint Military Pay System," February 15, 2001, stated that general controls over the subject system at DISA and the Defense Finance and Accounting Service were not adequate. The controls did not provide reasonable assurance of the integrity, confidentiality, and availability of computer-processed data.

4. Inspector General, DoD, Report No. D-2001-101, "Controls over Electronic Document Management," April 16, 2001, stated that management controls were not adequate to ensure the accuracy of electronic transactions using Electronic Document Management.

5. Inspector General, DoD, Report No. D-2001-095, "Controls for the Electronic Data Interchange at the Defense Finance and Accounting Service Columbus," April 6, 2001, stated that management controls could not ensure that the security for Electronic Data Access and Electronic Data Interchange were adequate.

6. Inspector General, DoD, Report No. D-2001-044, "Accreditation Policies and Information Technology Controls at the Defense Enterprise Computing Center Mechanicsburg," February 9, 2001, stated that management controls for the Mechanicsburg Center could not provide reasonable assurance of the adequacy of selected information system controls. The report further stated that DISA site recertification and reaccreditation decisions could be unreliable and inconsistent among DISA sites.

7. Inspector General, DoD, Report No. D-2001-029, "General Controls Over the Electronic Document Access System," December 27, 2000, stated that management controls were not adequate to ensure the accuracy of electronic transactions using Electronic Document Access.

8. Inspector General, DoD, Report No. D-2001-019, "Program Management of the Defense Security Service Case Control Management System," December 15, 2000, stated that management controls were inadequate for the acquisition of the Case Control Management Systems and the Defense Security Service Enterprise System.

9. Inspector General, DoD, Report No. D-2001-017, "Unclassified but Sensitive Internet Protocol Router Network Security Policy," December 12, 2000, stated that the lack of NIPRNet security policy guidelines was a material management control weakness.

10. Inspector General, DoD, Report No. D-2000-182, "Data Processing Controls Issues for the FY 1999 Military Retirement Fund," August 31, 2000, identified general control weaknesses in electronic data processing controls at the computer processing locations servicing the Military Retirement Fund. Control weaknesses included deficiencies in the design and operation of access controls, security policies and procedures, and program change control.

11. Inspector General, DoD, Report No. D-2000-142, "Defense Information Systems Agency's Acquisition Management of the Global Combat Support System," June 9, 2000, stated that management controls were inadequate. DISA had not integrated cost, schedule, and performance parameters into its management control plan for the acquisition of GCCS. Specifically, control objectives and techniques and evaluations for monitoring results and effectiveness did not link to mission area planning, budgeting, project management, accounting, and auditing cycles.

12. Inspector General, DoD, Report No. D-2000-139, "Controls Over the Integrated Accounts Payable Systems," June 5, 2000, stated that the DFAS controls over the subject system and the processing of vendor payments were not adequate to ensure that all payments were properly supported and valid.

13. Inspector General, DoD, Report No. D-2000-122, "Information Assurance in the Advanced Logistics Program," May 12, 2000, stated that management controls were not adequate to ensure that information assurance was properly addressed and evaluated during the development of the Advanced Logistics Program.

14. Army Audit Agency Report No. AA 01-319, "Corps of Engineers Financial Management System: General and Application Controls," June 26, 2001, stated that internal controls over the Corps of Engineers' Financial Management System were not adequate to rely on for the Civil Works Program financial statements. The Corps did not have a reliable set of computer controls to ensure the integrity, confidentiality, and availability of financial and sensitive data contained in the system.

15. Army Audit Agency Report No. AA 00-286, "Information Assurance—Phase IV: Reporting Process and Vulnerability Assessment Results," June 30, 2000, stated that information systems at 15 locations had significant host-level vulnerabilities. Poor configuration management controls allowed locally owned systems and networks to have root access to Army information systems.

16. Naval Audit Service Report No. N2001-0029, "Department of the Navy Principal Statements for FY 2000: Feeder Systems and Interfaces," June 1, 2001, identified material internal control weakness, including incomplete contract files and insufficient audit trails at three Naval Supply Systems Command activities. Without audit trails, the Navy could not verify that data was accurate, complete, and supportable, as required by the Financial Management Regulation.

17. Naval Audit Service Report No. N2000-0045, "Navy Capital Working Fund Financial Management Feeder Systems for FY 1999," September 29, 2000, identified material internal control weaknesses for the Department of Navy Capital Working Fund. The weaknesses included inadequate control of access, failure to ensure backup and disaster recovery, and insufficient and outdated system documentation.

18. Air Force Audit Agency Report No. 99066040, "Air Force Research Laboratory UNIX-Based Computer Systems," May 21, 2001, stated that computer system personnel did not require adequate technical and management controls for continued security over Air Force Research Laboratories systems and information.

19. Air Force Audit Agency Report No. 00054006, "Air Force Restoration Information Management Systems Controls," May 18, 2001, stated that system control weaknesses were identified for 6 of 11 control areas reviewed. Managers of the Air Force Restoration Information Management System had not established adequate system password and data access controls or ensured that the system provided a transaction history and audit trails.

20. Air Force Audit Agency Report No. 99066038, "Web Page Management," November 8, 2000, identified management control weaknesses for web pages, establishing web master core training requirements, and enhancing web server security.

21. Air Force Audit Agency Report No. 99054027, "Review of Controls in the Command Online Accounting and Reporting System (COARS)," November 1, 2000, stated that general controls for the subject system did not meet financial management system requirements. The system did not meet requirements for separation of duties, access controls, system software, and physical security. The Air Force had no assurance that the system applications were running in a secure, controlled environment.

22. Air Force Audit Agency Report No. 99066018, "Information Assurance—Implementing Controls Over Known Vulnerabilities in Pacific Air Force Computer Systems," August 11, 2000, identified weaknesses for the Pacific Air

Force computer systems in configuration management controls. Controls did not ensure that current vendor patches and service packs were loaded on all computers and that users were assigned proper privileges. In addition, identification and authentication controls to prevent unauthorized access to information on networked computers were weak.

23. Air Force Audit Agency Report No. 99066028, "Controls Within the Acquisition Due-In System," May 1, 2000, identified control weaknesses for the Acquisition Due-In System in access controls, transaction histories and audit trails, transaction controls, completeness controls, and documentation.

Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense, Deputy Chief Information Officer
  Deputy Assistant Secretary of Defense, Security and Information Operations
    Director, Defense-Wide Information Assurance Program

Joint Staff

Director, Joint Staff
  Director, Operations
    Deputy Director for Operations (Information Operations)
  Director, Command, Control, Communications, and Computers
    Chief, Information Assurance Division, Deputy Director for Command, Control, Communications, and Computers Assessment and Technology

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief Information Officer, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Navy Chief Information Officer
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Department of the Air Force
Auditor General, Department of the Air Force

Other Defense Organizations

Commander, Joint Task Force Computer Network Defense
Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations

Office of Management and Budget
  Office of the Information and Regulatory Affairs
  National Security Division
General Accounting Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Evaluation Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector, General DoD, who contributed to the report are listed below.

Mary L. Ugone
Wanda A. Hopkins
Robert K. West
Judith I. Padgett
Bryon J. Farber
Richard B. Vasquez
Heather L. Jordan
Mandy L. Rush
Henry D. Barton
Dharam V. Jain
Ann Ferrante
Jacqueline N. Pugh

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: FY 2001 DOD Information Security Status for Government Information Security Reform

B. DATE Report Downloaded From the Internet: 11/01/01

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 11/01/01**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.